Received January 27, 2020, accepted February 27, 2020, date of publication March 10, 2020, date of current version March 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2979848

Improving Physical Layer Security of Cellular Networks Using Full-Duplex Jamming Relay-Aided D2D Communications

MAJID H. KHOSHAFA[1], (Student Member, IEEE), TELEX M. N. NGATCHED[1], (Senior Member, IEEE), MOHAMED H. AHMED[2], (Senior Member, IEEE), AND AHMED IBRAHIM[1], (Member, IEEE)

[1]Department of Electrical and Computer Engineering, Memorial University of Newfoundland, St. John's, NL A1B 3X5, Canada
[2]School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada

Corresponding author: Majid H. Khoshafa (mhakhoshafa@mun.ca)

This work was supported by NSERC-Canada through Discovery Grant No. 2014-03638.

ABSTRACT This paper investigates the physical layer security and data transmission in cellular networks with inband underlay Device-to-Device (D2D) communications, where there is no direct link between D2D users. We propose to apply full-duplex (FD) transmission and dual antenna selection at the D2D relay node. The relay node can simultaneously act as a friendly jammer to improve the secrecy performance of the cellular network while enhancing the D2D communication data transmission. This is an appealing and practical scheme where spectrum sharing is beneficial for the D2D and cellular networks in terms of reliability enhancement and security provisioning, respectively. The practical scenario, where the eavesdropper is passive, is considered. The eavesdropper uses either selection combining or maximal ratio combining to combine the wiretapped signals of the cellular network. The secrecy performance of the cellular network is analyzed, and closed-form expressions for the secrecy outage probability and the probability of non-zero secrecy capacity are derived. We show that increasing the number of FD jamming antennas enhances the secrecy performance of the cellular network. A closed-form expression of the D2D outage probability is also provided. Simulation and numerical results are provided to verify the efficiency of the proposed scheme and to validate the accuracy of the derived expressions.

INDEX TERMS Physical layer security, D2D communication, full-duplex relay, jamming, secrecy outage probability.

I. INTRODUCTION

Device-to-Device (D2D) communication, which enables proximate user pairs to communicate directly rather than through the base station (BS), has received considerable attention as one of the main technologies in the fifth-generation (5G) cellular communications [1]. The advantages of D2D communications are multi-fold and include increased spectrum efficiency, shortened transmission latency, increased cellular coverage, and increased energy efficiency [2]. D2D communication also offers new mobile service advantages for several proximity-based services such as multi-player gaming, social networking, and content sharing [3]. According to the spectrum band utilization, D2D communication can be classified into two approaches; inband D2D and out-band D2D communications. In the first approach, the same spectrum band is shared between the cellular network and the D2D communication [2], whereas in the second approach, the D2D network utilizes the unlicensed spectrum band [3]. The inband D2D communication can also be classified into two categories, namely, underlay and overlay D2D communication. In underlay D2D communication, both D2D and cellular users use the same frequencies, and hence, interference management is necessary. In overlay D2D communication, the cellular spectrum is split into non-overlapping frequency sets, where one set is allocated to D2D users, while the other is allocated to the cellular users. Therefore, interference management between D2D users cellular users is not needed to overlay D2D communication. More importantly, underlay D2D communications

The associate editor coordinating the review of this manuscript and approving it for publication was Chunlong He.

can play a primary role in improving cellular network security. In this case, the D2D users can be used as friendly jammers to enhance the secrecy performance of the cellular network, while the cellular network shares its spectrum with the D2D users in return.

From the information theoretic perspective, as an alternative/supplement to complicated cryptographic approaches, physical layer security (PLS), initially investigated by Wyner [4], has seen a surge of interest as a leading technique to increase the security level for the wireless communication systems against eavesdropping attacks. PLS utilizes the natural properties of communication channels and noise to limit the data that can be leaked at the bit level by unintended receivers or devices. The main advantages of PLS are that it is simple, does not require any computational restrictions on the eavesdroppers, and can operate independently of higher layers [5]. Relaying and diversity technologies have been widely adopted to improve the PLS of cellular networks [6]. Many techniques, such as cooperative beamforming [7], artificial noise [8], and multi-antenna beamforming [9], have been investigated to degrade the quality of the wiretapped signals at the eavesdropper. Moreover, cooperative jamming (CJ) has been extensively studied to safeguard wireless communications. In CJ, a relay terminal is chosen by the authorized receiver to degrade the eavesdroppers signal by sending a jamming signal [10], [11]. In cooperative scenarios, CJ and cooperative relaying [12], [13] are considered as promising techniques to efficiently increase the secrecy capacity. Furthermore, the PLS of cooperative systems, such as non-orthogonal multiple access networks, is investigated in [14]–[17].

In cellular networks with inband underlay D2D communication, the interference generated by the spectrum sharing between cellular communications and D2D communication is considered as one of the most crucial problems. Such interference is traditionally considered as a drawback that leads to performance degradation of the cellular network. Thus, earlier works on D2D communication focused on decreasing the interference effects in cellular networks by interference management techniques. The underlying assumption in these works is that the interference generated as a result of the spectrum sharing is harmful, and needs to be mitigated, suppressed, or avoided by several techniques. However, as recently proposed in [18]–[20], from a PLS perspective, such interference could be beneficial as it can be utilized as artificial noise in CJ to paralyze malicious eavesdroppers and help the cellular users (CUs) prevent wiretapping. This is possible provided that the interference to the CUs is less severe than that to the eavesdroppers. In contrast to the friendly jammer, which consumes power merely to confound the eavesdroppers, D2D communication can further transmit the confidential signal simultaneously, achieving a win-win situation between the D2D users and the CUs. In [21], the influence of the resource allocation on the secrecy capacity is studied to achieve the minimum secrecy rate. Towards this end, the authors of [22] investigate the selection of the appropriate D2D pairs based on the distance between CUs and D2D pairs to confuse the eavesdroppers.

On the other development, full-duplex (FD) communications, which allows the concurrent transmission and reception on a specific spectrum band, has attracted lots of attention as a result of its potential to increase the spectrum efficiency compared to half-duplex communications. Due to the recent advances in the field of signal processing and antenna technology [23], FD transmission, which was previously considered impractical and difficult to implement because of the associated self-interference (SI), is now a convenient choice in various applications. Interestingly, this evolution on FD transmission presents new advantages in safeguarding wireless networks [24]. From a secrecy performance perspective, FD jamming receiver is investigated in [25]. Motivated by this observation, recent research works have studied the inband D2D communication from the PLS perspective [22], [26]. To enhance the PLS performances of cellular networks, these works study the potentials of inband D2D communication, but only consider the case where there is a direct link between D2D users [27]. However, in some scenarios, the link condition and proximity may not be beneficial for direct communication. In such scenarios, the performance of D2D communication could be enhanced by employing network-assisted transmission through relays. This approach, referred to as relay-aided D2D communication, can efficiently provide a better quality of service between remote D2D pairs. The PLS of underlay multihop D2D relaying is investigated in [28], but from the perspective of enhancing the secrecy performance of D2D links only. It is important to note that, by adopting the FD operation for jamming, the cellular can have secure transmission during the two phases of the D2D transmission. This is in contrast with the work in [29] where, due to the absence of FD, the cellular user can only transmit during the second phase of the D2D transmission for improved secrecy, which negatively impact its spectral efficiency.

In this paper, we study the PLS of FD relay-aided underlay D2D communication and propose a dual antenna selection to enhance the secrecy performance of the cellular network and increase the reliability in the D2D communication concurrently. This is achieved by equipping the relay with FD multiple-input multiple-output (MIMO) antennas. Antenna selection approach is employed in this work to avoid the high hardware complexity while maintaining the diversity and reliability advantages from multiple antennas. In the proposed scheme, the data antenna selection at the relay is utilized to increase the reliability of D2D communications, whereas the jamming antenna selection is used to confound the eavesdropper. Thus, the secrecy capacity of the cellular network is maximized. Thanks to the FD dual antenna selection at the relay, the secrecy and data transmission performance are improved concomitantly. Compared to our earlier work in [30], in addition to the selection combining (SC) technique, the maximum ratio combining (MRC) technique, which is considered the worst case as it results in the lowest secrecy performance of the cellular network when employed at the

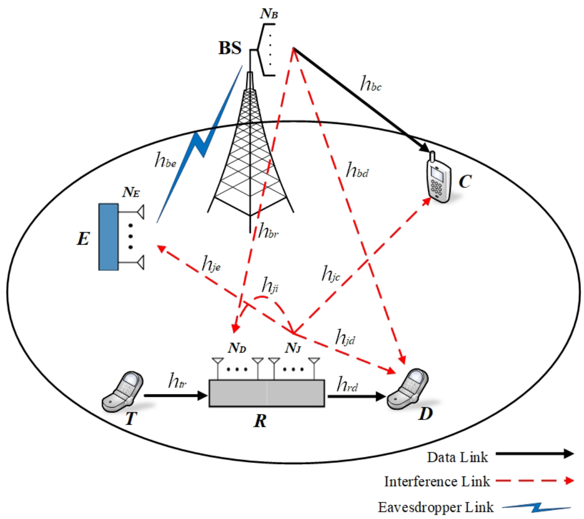


FIGURE 1. System model.

eavesdropper, is also investigated. In this respect, the impact of the multiple antennas, at the base station and eavesdropper, on the secrecy performance of the cellular network is studied. In doing so, jamming antenna selection strategy is utilized in this work to maintain the reliability and diversity benefits from multiple antennas while avoiding the high hardware complexity and signaling overheads.

The main contributions of this paper can be summarized as follows:

- A new network-assisted inband underlay D2D communication system is introduced, where an FD MIMO relay, in addition to its ability to improve data rate, is also used as a friendly jammer.
- A dual antenna selection at the FD MIMO relay is proposed to improve the data transmission of the D2D communication and enhance the secrecy capacity of the cellular network simultaneously.
- The secrecy performance of the cellular network is analyzed and closed-form expressions of the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity (PNSC) are derived. Additionally, the outage probability of the D2D communication is investigated, and an analytical expression is also obtained.
- Concise expressions for the asymptotic SOP for the cellular network are provided in the high transmit power regime. These expressions reveal that SC and MRC achieve the same secrecy diversity order.
- Monte-Carlo simulations results are presented and compared with the derived analytical expressions, verifying and confirming the correctness and accuracy of the latter.

The remainder of the paper is arranged as follows. In Section II, the proposed system model is described. Section III studies the performance analysis of the proposed inband underlay FD relay D2D communication system. The main results are summarized and discussed in Section IV. Finally, Section V concludes the paper.

TABLE 1. Table of symbols.

Symbols	Description
P_B	Transmission power of BS
P	Transmission power of D2D users
P_{R_j}	Jamming power
y_a	Received signal at node a
σ_a^2	Variance of AWGN at node a
n_a	AWGN at node a
$\mathcal{U}_i^1$	Selected receiving antenna at R
$\mathcal{U}_i^2$	Selected transmitting antenna at R
R_j	Selected jamming antenna
N_J	Number of jamming antennas at R
N_D	Number of data antennas at MIMO relay
N_E	Number of antennas at E
h_{ab}	Channel coefficient of ab link
λ_{ab}	Mean of the channel gain
x_d	D2D signal
x_b	BS transmitted signal
x_j	Jammimg signal
γ_a	SINR at node a
$\bar{\gamma}_a$	Average SNR at node a
γ_{D2D}	End-to-end SINR of the D2D link
γ_{up}	Upper bound SINR of the D2D link
C_S	Secrecy capacity
C_C	Cellular capacity
C_E	Eavesdropper capacity
P_{out}	Outage probability for D2D link
SOP	Secrecy outage probability for cellular link
SOP$^\infty$	Asymptotic secrecy outage probability for cellular link
$\mathcal{R}_d$	D2D required data rate
$\mathcal{R}_s$	Target secrecy rate of cellular link
$\mathbb{E}[.]$	Expectation operator
$f_X(.)$	PDF of random variable X
$F_X(.)$	CDF of random variable X
$F_X^\infty(.)$	Asymptotic CDF of random variable X
Pr(.)	Probability of an event
$\mathcal{G}$	Relaying gain
G_a	Secrecy diversity order
G_d	Secrecy array gain
μ_1	$\bar{\gamma}_r\lambda_{tr}$
μ_2	$\bar{\gamma}_d\lambda_{rd}$
μ_3	$\bar{\gamma}_{bd}\lambda_{bd}$
ω_1	$\bar{\gamma}_c\lambda_{bc}$
ω_2	$\bar{\gamma}_{jc}\lambda_{jc}$
ω_3	$\bar{\gamma}_e\lambda_{be}$
ω_4	$\bar{\gamma}_{je}\lambda_{je}$
φ	$2^{2\mathcal{R}_d-1}$
β	$2^{\mathcal{R}_s}$
α	$\beta - 1$

II. SYSTEM MODEL

As shown in Fig. 1, a downlink transmission scenario in a relay-aided D2D communication underlying cellular network, where the cellular network enables the D2D users to transmit simultaneously in the same spectral band in a specific environment, is considered. We consider a cellular network consisting of a multi-antenna base station (BS), equipped with N_B antennas, communicating with a single-antenna cellular user, C, in the presence of a passive multi-antenna eavesdropper, E, equipped with N_E antennas. The D2D network consists of a single-antenna D2D transmitter, T, a multi-antenna relay, R, and a single-antenna D2D receiver, D. The amplify-and-forward (AF) relay, R, operates in the FD mode and is equipped with N_D antennas for receiving data from T and transmitting to D, and N_J antennas for transmitting jamming signals towards E. We assume that the channel state information (CSI) of the wiretap channel is available at E, and that of the cellular channel is known to C. All other nodes operate in the half-duplex mode. Furthermore, the D2D transmissions require two phases, one for each hop.

In addition, all communication channels are assumed to undergo flat fading with Rayleigh distribution. In the first phase, T transmits the D2D signal to R. Next, the received signal at R is amplified and re-transmitted to D in the second phase. In both phases, R transmits a jamming signal to E to improve the cellular link security. It should be noted that the BS transmits to the cellular user in both phases as well. Thus, as a compensation for spectrum sharing, the D2D MIMO relay serves as a friendly jammer to ensure high-security level for the cellular network, and thus enables a win-win situation between the two networks, i.e., security provisioning for the cellular user and high reliability for the D2D users. We indicate $\mathcal{U}_i^1$ and $\mathcal{U}_i^2$ as the i^{th} receiving and transmitting antennas in the first and second phases, respectively, where $i = 1, \ldots, N_D$. In a similar manner, R_j denotes the jamming antenna, where $j = 1, \ldots, N_J$, and BS_l denotes the transmitting antenna in the BS, where $l = 1, \ldots, N_B$, The channel coefficients for the $T \to \mathcal{U}_i^1, \mathcal{U}_i^2 \to D$, $\mathrm{BS}_l \to C$, $\mathrm{BS}_l \to E$, $\mathrm{BS}_l \to D$, $R_j \to E$, $R_j \to C$, $R_j \to \mathcal{U}_i^1$, and $R_j \to D$ links are denoted as h_{tr}, h_{rd}, h_{bc}, h_{be}, h_{bd}, h_{je}, h_{jc}, h_{ji}, and h_{jd}, respectively. In addition, the channel power gains are indicated by $|h_{ab}|^2$, which are independent and exponentially distributed random variables with a mean of $\lambda_{ab} = \mathbb{E}[|h_{ab}|^2]$, where $\mathbb{E}$ is the expectation operator and $ab \in \{tr, rd, bc, be, bd, je, jc, ji, jd\}$. Furthermore, the variances of the additive white Gaussian noise (AWGN) at R, D, C, and E are denoted by $\sigma_r^2, \sigma_d^2, \sigma_c^2$, and σ_e^2, respectively. It is assumed that the wiretap channel gain is not available at the BS and R. It is also assumed that T and R are transmitting with equal power P.

During the first phase, the receiving antenna $\mathcal{U}_i^1$ is chosen to maximize the instantaneous SNR at R. As a result of using FD relaying, R receives data from T and transmits jamming signals to E at the same time. Since the modern technology can considerably suppress the self-interference to the noise level [31], it can be assumed that the residual self-interference is negligible. The received signal at the i^{th} receiving antenna, $\mathcal{U}_i^1$, is given by

$$y_R = \sqrt{P}\, h_{tr}\, x_d + \sqrt{P_B}\, h_{br}\, x_b + n_r, \tag{1}$$

where x_d and x_b are the D2D and BS transmission signals, respectively, P and P_B are the D2D and BS transmission power, respectively, and n_r is the AWGN at the MIMO relay. During the second phase, the transmitting antenna $\mathcal{U}_i^2$ is chosen to maximize the instantaneous SNR at D. Then $\mathcal{U}_i^2$ transmits an amplified version of the received signal to D after employing the relaying gain $\mathcal{G}$. Hence, the received signal at D is given by

$$\begin{aligned} y_D = {} & \mathcal{G}\, h_{rd} \left(\sqrt{P}\, h_{tr}\, x_d + \sqrt{P_B}\, h_{br}\, x_b + n_r\right) \\ & + \sqrt{P_B}\, h_{bd}\, x_b + \sqrt{P_{Rj}}\, h_{jd}\, x_j + n_d, \end{aligned} \tag{2}$$

where x_j is the jamming signal, P_{Rj} is the jamming transmitted power, and n_d is the AWGN at D. However, since the jamming power P_{Rj} and coefficient h_{jd} are assumed to be known at D, the interference at D generated by the jamming antenna can be eliminated through digital interference cancellation [32]. During each phase, the received signal at C is given by

$$y_C = \sqrt{P_B}\, h_{bc}\, x_b + \sqrt{P_{Rj}}\, h_{jc}\, x_j + n_c, \tag{3}$$

where n_c is the AWGN at C. In a similar manner, the received signal at E during each phase is given by

$$y_E = \sqrt{P_B}\, h_{be}\, x_b + \sqrt{P_{Rj}}\, h_{je}\, x_j + n_e, \tag{4}$$

where n_e is the AWGN at the E. In (3) and (4), it is assumed that the interference from T is negligible. This widely used assumption can be justified by the fact that T is far away and transmits with low power [33], [34]. As the jamming transmitted power from R_j is higher than the data transmitted power from $\mathcal{U}_i^2$, we assume that the interference from $\mathcal{U}_i^2$ towards C is negligible. This assumption is necessary to get mathematically tractable closed-form expressions. For AF relaying scheme, the relaying gain $\mathcal{G}$ is given by [35], [36]

$$\mathcal{G} = \sqrt{\frac{P}{P\,|h_{tr}|^2 + P_B\,|h_{br}|^2 + \sigma_r^2}}. \tag{5}$$

Substituting (5) into (2), the instantaneous end-to-end signal-to-interference-and-noise ratio (SINR) for the D2D link, γ_{D2D}, can be derived as

$$\gamma_{\mathrm{D2D}} = \frac{\mathcal{G}^2 P\,|h_{tr}|^2\,|h_{rd}|^2}{\mathcal{G}^2\,|h_{rd}|^2\left(P_B\,|h_{br}|^2 + \sigma_r^2\right) + P_B\,|h_{bd}|^2 + \sigma_d^2}, \tag{6}$$

which, after some algebraic manipulations, simplifies to

$$\gamma_{\mathrm{D2D}} = \frac{\gamma_R\,\gamma_D}{\gamma_R + \gamma_D + 1}, \tag{7}$$

where γ_R and γ_D are the SINR at R and D, respectively. The SINR at R is given by

$$\gamma_R = \frac{P\,|h_{tr}|^2}{\sigma_r^2 + P_b\,|h_{br}|^2} = \frac{\gamma_{tr}}{1 + \gamma_{br}}, \tag{8}$$

and the SINR at D is given by

$$\gamma_D = \frac{P\,|h_{rd}|^2}{\sigma_d^2 + P_b\,|h_{bd}|^2} = \frac{\gamma_{rd}}{1 + \gamma_{bd}}, \tag{9}$$

where $\gamma_{tr} = \bar{\gamma}_{tr}\,|h_{tr}|^2$, $\gamma_{br} = \bar{\gamma}_{br}\,|h_{br}|^2$, $\bar{\gamma}_r = \frac{P}{\sigma_r^2}$, and $\bar{\gamma}_{br} = \frac{P_B}{\sigma_r^2}$. Similarity, $\gamma_{rd} = \bar{\gamma}_{rd}\,|h_{rd}|^2$, $\gamma_{bd} = \bar{\gamma}_{bd}\,|h_{bd}|^2$, $\bar{\gamma}_{rd} = \frac{P}{\sigma_d^2}$, and $\bar{\gamma}_{bd} = \frac{P_B}{\sigma_d^2}$. Let us define $\mu_1 = \bar{\gamma}_{tr}\lambda_{tr}$, $\mu_2 = \bar{\gamma}_{br}\lambda_{br}$, $\mu_3 = \bar{\gamma}_{rd}\lambda_{rd}$, and $\mu_4 = \bar{\gamma}_{bd}\lambda_{bd}$.

The maximum D2D two-hop channel gain can be calculated as follows

$$|h_\upsilon|^2 = \arg \max_{i=1,..N_D} \left|h_{\upsilon_i}\right|^2, \tag{10}$$

where $\upsilon \in \{tr, rd\}$. The probability density function (PDF) of $|h_\upsilon|^2$ is given by [37]

$$f_{|h_\upsilon|^2}(\gamma) = \frac{N_D}{\lambda_\upsilon}\, e^{-\frac{\gamma}{\lambda_\upsilon}} \left(1 - e^{-\frac{\gamma}{\lambda_\upsilon}}\right)^{N_D - 1}. \tag{11}$$

III. PERFORMANCE ANALYSIS

In this section, a comprehensive performance analysis of the illustrated system model is presented. Specifically, closed-form expressions are derived for essential performance metrics, i.e., the D2D outage probability, the SOP, and the PNSC. Additionally, the benefits of the cooperative system model are examined. It is noteworthy that a passive eavesdropper is considered, where the eavesdropper channel states are not known to BS and R.

A. D2D OUTAGE PROBABILITY

The outage probability of the D2D communication, P_{out}, can be expressed as

$$P_{out} = \Pr\left(\gamma_{D2D} \leq \varphi\right), \tag{12}$$

where $\varphi = 2^{2\mathcal{R}_d} - 1$, γ_{D2D} is the end-to-end SINR for the D2D link, and $\mathcal{R}_d$ is the D2D required data rate. However, the expression in (7) is not mathematically tractable.

As a result, a tight upper bound γ_{up} is used to express the end-to-end SINR of the $T \rightarrow R \rightarrow D$ link as follows [38], [39]

$$\gamma_{D2D} \leq \gamma_{up} \triangleq \min\left(\gamma_R, \gamma_D\right). \tag{13}$$

Thus, P_{out} can be expressed as

$$\begin{aligned} P_{out} &= \Pr\left(\gamma_{up} \leq \varphi\right) \\ &= \Pr\left(\min\left(\gamma_R, \gamma_D\right) \leq \varphi\right) \\ &= 1 - \left(1 - F_{\gamma_R}(\varphi)\right)\left(1 - F_{\gamma_D}(\varphi)\right), \end{aligned} \tag{14}$$

where $F_{\gamma_R}(.)$ and $F_{\gamma_D}(.)$ are the cumulative distribution functions (CDFs) of γ_R and γ_D, respectively. We can determine the PDF of γ_R as [40]

$$f_{\gamma_R}(\gamma) = \int_0^\infty (y+1) f_{\gamma_{tr}}(\gamma(y+1)) f_{\gamma_{br}}(y)dy, \tag{15}$$

where $f_{\gamma_{tr}}(.)$ is given by

$$f_{\gamma_{tr}}(\gamma) = \frac{N_D}{\mu_1} e^{-\frac{\gamma}{\mu_1}} \left(1 - e^{-\frac{\gamma}{\mu_1}}\right)^{N_D - 1}. \tag{16}$$

The PDF of γ_{tr} in (16) can be expressed in terms of the binomial expansion [41, eq. (1.111)] as

$$f_{\gamma_{tr}}(\gamma) = \frac{N_D}{\mu_1} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D - 1}{k} e^{-\frac{\gamma(k+1)}{\mu_1}}, \tag{17}$$

and $f_{\gamma_{br}}(.)$ is given by

$$f_{\gamma_{br}}(x) = \frac{1}{\mu_2} e^{-\frac{x}{\mu_2}}. \tag{18}$$

By substituting (17) and (18) in (15), and after simple algebraic manipulations, the PDF of γ_R is derived as

$$f_{\gamma_R}(\gamma) = \frac{N_D}{\mu_1 \mu_2} \sum_{k=0}^{N_D-1} (-1)^k \binom{N_D - 1}{k} \times e^{-\frac{\gamma(k+1)}{\mu_1}} \left(\frac{1 + \frac{\gamma(k+1)}{\mu_1} + \frac{1}{\mu_2}}{\left(\frac{\gamma(k+1)}{\mu_1} + \frac{1}{\mu_2}\right)^2} \right). \tag{19}$$

From (19), $F_{\gamma_R}(\gamma)$ can be easily obtained as

$$F_{\gamma_R}(\gamma) = N_D \sum_{k=0}^{N_D-1} (-1)^k \frac{\binom{N_D-1}{k}}{(k+1)} \times \left(1 - \frac{e^{-\frac{\gamma(k+1)}{\mu_1}}}{\left(1 + \frac{\gamma(k+1)\mu_2}{\mu_1}\right)}\right). \tag{20}$$

Following the same steps in the derivation of (20), $F_{\gamma_D}(\gamma)$ can be obtained as

$$F_{\gamma_D}(\gamma) = N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{(k+1)} \times \left(1 - \frac{e^{-\frac{\gamma(k+1)}{\mu_3}}}{\left(1 + \frac{\gamma(k+1)\mu_4}{\mu_3}\right)}\right). \tag{21}$$

By substituting (20) and (21) in (14), P_{out} can be obtained as in (22) at the bottom of the next page.

B. SECRECY OUTAGE PROBABILITY

The SOP can be defined as the probability that the achievable secrecy rate is less than a predefined target secrecy rate, $\mathcal{R}_s$, for the cellular transmission. Based on this, the SOP is given by [42]

$$\text{SOP} = \Pr\left(C_S < \mathcal{R}_s\right), \tag{23}$$

where the secrecy capacity, normalized to a unit bandwidth, C_S, is given by [43]

$$C_S = \begin{cases} C_C - C_E, & \gamma_C > \gamma_E, \\ 0, & \gamma_C \leq \gamma_E, \end{cases} \tag{24}$$

where C_C and C_E are the cellular and eavesdropper capacities normalized to a unit bandwidth, respectively, and γ_C and γ_E are the SINR at C and E, respectively. In this respect, C_C can be obtained by

$$C_C = \log_2\left(1 + \gamma_C\right) = \log_2\left(1 + \frac{\gamma_{bc}}{1 + \gamma_{jc}}\right), \tag{25}$$

where $\gamma_{bc} = \bar{\gamma}_c \left|h_{bc}\right|^2$, $\gamma_{jc} = \bar{\gamma}_{jc} \left|h_{jc}\right|^2$, $\bar{\gamma}_c = \frac{P_B}{\sigma_c^2}$, and $\bar{\gamma}_{jc} = \frac{P_j}{\sigma_c^2}$. Let us define $\omega_1 = \bar{\gamma}_c \lambda_{bc}$, and $\omega_2 = \bar{\gamma}_{jc} \lambda_{jc}$. In addition, C_E can be obtained by

$$C_E = \log_2\left(1 + \gamma_E\right) = \log_2\left(1 + \frac{\gamma_{be}}{1 + \gamma_{je}}\right), \tag{26}$$

where $\gamma_{be} = \bar{\gamma}_e \left|h_{be}\right|^2$, $\gamma_{je} = \bar{\gamma}_{je} \left|h_{je}\right|^2$, $\bar{\gamma}_e = \frac{P_B}{\sigma_e^2}$, and $\bar{\gamma}_{je} = \frac{P_j}{\sigma_e^2}$. Let us define $\omega_3 = \bar{\gamma}_e \lambda_{be}$, and $\omega_4 = \bar{\gamma}_{je} \lambda_{je}$.

Jamming Antenna Selection Approach: Because the channel gains between the jamming antennas, R_j, and the eavesdropper, E, are not available, the jamming antenna is selected based on the minimum interference generated towards C, since the channel gain between R_j and C is assumed to be known at R. In this case, the Eavesdropper would see a random signal from the selected jamming antenna. Thus, the jamming antenna selection is chosen to satisfy

$$\left|h_{jc}\right|^2 = \min_{i=1,..N_J} \left|h_{jc_i}\right|^2. \tag{27}$$

On the other hand, E would see random channels h_{be} and h_{je}, from selected antennas at BS and R, respectively. At E, two practical diversity combining techniques, SC and MRC, are investigated. It should be noted that the selected antenna R_j at R transmits a jamming signal to confuse E.

1) EAVESDROPPER's CHANNEL WITH SC

In this technique, the signal with the highest instantaneous SNR is selected. For the SC approach, the PDF of γ_E can be derived using

$$f_{\gamma_E}^{\mathrm{SC}}(x) = \int_0^\infty (y+1) f_{\gamma_{be}}(x(y+1)) f_{\gamma_{je}}(y) dy, \tag{28}$$

where $f_{\gamma_{be}}(.)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{N_E}{\omega_3} \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E-1}{k} e^{-\frac{\gamma(k+1)}{\omega_3}}. \tag{29}$$

and $f_{\gamma_{je}}(.)$ is given by

$$f_{\gamma_{je}}(\gamma) = \frac{1}{\omega_4} e^{-\frac{\gamma}{\omega_4}}. \tag{30}$$

By substituting (29) and (30) in (28), and after simple algebraic manipulations, $f_{\gamma_E}^{\mathrm{SC}}(\gamma)$ is obtained as

$$f_{\gamma_E}^{\mathrm{SC}}(\gamma) = \frac{N_E}{\omega_3\, \omega_4} \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E-1}{k} e^{-\frac{\gamma(k+1)}{\omega_3}} \times \left(\frac{1 + \frac{\gamma(k+1)}{\omega_3} + \frac{1}{\omega_4}}{\left(\frac{\gamma(k+1)}{\omega_3} + \frac{1}{\omega_4}\right)^2} \right). \tag{31}$$

The SOP for SC, $\mathrm{SOP_{SC}}$, can be formulated as

$$\mathrm{SOP_{SC}} = \int_0^\infty F_{\gamma_C}(\beta\gamma + \alpha) f_{\gamma_E}^{\mathrm{SC}}(\gamma)\, d\gamma. \tag{32}$$

Lemma 1: The $\mathrm{SOP_{SC}}$ can be obtained as in (33) at the bottom of this page, where $\beta = 2^{\mathcal{R}_s}$, $\alpha = \beta - 1$, $\mathcal{A}_1 = \frac{\omega_2(s+1)}{\omega_1}$, $\mathcal{A}_2 = \frac{(s+1)\beta}{\omega_1} + \frac{k+1}{\omega_3}$, $\mathcal{A}_3 = \frac{\omega_3}{(k+1)\omega_4}$, $\mathcal{A}_4 = \frac{(k+1)}{\omega_3}\left(N_j + \mathcal{A}_1\alpha\right) - \frac{\mathcal{A}_1\beta}{\omega_4}$, and Ei(.) is the exponential integral function [41, eq. (8.21.1)].

Proof: See Appendix. ■

2) EAVESDROPPER's CHANNEL WITH MRC

In this technique, the received signals are coherently combined. The PDF of γ_E for MRC can be obtained as

$$f_{\gamma_E}^{\mathrm{MRC}}(x) = \int_0^\infty (y+1) f_{\gamma_{be}}(x(y+1)) f_{\gamma_{je}}(y) dy, \tag{34}$$

$$P_{out} = N_D \sum_{k=0}^{N_D-1} \frac{(-1)^k \binom{N_D-1}{k}}{k+1} \left[\left(2 - \frac{e^{-\frac{\varphi(k+1)}{\mu_1}}}{\left(1 + \frac{\varphi(k+1)\mu_2}{\mu_1}\right)} - \frac{e^{-\frac{\varphi(k+1)}{\mu_3}}}{\left(1 + \frac{\varphi(k+1)\mu_4}{\mu_3}\right)} \right) - N_D \sum_{m=0}^{N_D-1} \frac{(-1)^m}{m+1} \times \binom{N_D-1}{m} \left(\left(1 - \frac{e^{-\frac{\varphi(k+1)}{\mu_1}}}{\left(1 + \frac{\varphi(k+1)\mu_2}{\mu_1}\right)} \right) \left(1 - \frac{e^{-\frac{\varphi(m+1)}{\mu_3}}}{\left(1 + \frac{\varphi(m+1)\mu_4}{\mu_3}\right)} \right) \right) \right]. \tag{22}$$

$$\begin{aligned}\mathrm{SOP_{SC}} = {} & \frac{N_E\, N_B}{\omega_3\omega_4} \sum_{k=0}^{N_E-1} \sum_{s=0}^{N_B-1} \frac{(-1)^k}{(k+1)} \binom{N_E-1}{k} \binom{N_B-1}{s} \left[\left(\frac{\omega_3\omega_4}{(k+1)} - N_J e^{\frac{(s+1)\alpha}{\omega_1}} \right.\right. \\ & \times \left(\frac{1}{\mathcal{A}_4} \left(\frac{\omega_3\mathcal{A}_2}{(k+1)} e^{\mathcal{A}_2\mathcal{A}_3} \mathrm{Ei}\left[-\mathcal{A}_2\mathcal{A}_3\right] + \frac{1}{\mathcal{A}_3} + \frac{\left(\frac{k+1}{\omega_3}\right)\left(N_J + \mathcal{A}_1\alpha\right) - \mathcal{A}_1\beta\left(1 + \frac{1}{\omega_4}\right)}{\mathcal{A}_4} \right.\right. \\ & \left.\left.\left.\left.\left. \times \left(-e^{\mathcal{A}_2\mathcal{A}_3} \mathrm{Ei}\left[-\mathcal{A}_2\mathcal{A}_3\right] + e^{\frac{\mathcal{A}_2(N_J+\mathcal{A}_1\alpha)}{\mathcal{A}_1\beta}} \mathrm{Ei}\left[-\frac{\mathcal{A}_2(N_J+\mathcal{A}_1\alpha)}{\mathcal{A}_1\beta} \right] \right) \right) \right) \right) \right],\end{aligned} \tag{33}$$

$$\begin{aligned}\mathrm{SOP_{MRC}} = {} & \frac{N_B}{\Gamma(N_E)\,\omega_3^{N_E}\omega_4} \sum_{m=0}^{N_E} \sum_{q=0}^{N_B-1} \frac{(-1)^q \binom{N_E}{k}\binom{N_B-1}{q}\Gamma(m+1)}{(q+1)} \left[\omega_3^{N_E} e^{\frac{1}{\omega_4}} \sum_{p=0}^{N_E-1} \binom{N_E-1}{p} \right. \\ & \times \left(\frac{-1}{\omega_4}\right)^{N_E-1-p} \Gamma\left(p-m, \frac{1}{\omega_4}\right) - \frac{N_J\, \omega_1\omega_3^{m+1} e^{-\frac{(q+1)\alpha}{\omega_1}}}{\omega_2(q+1)\beta} \left(\sum_{i=1}^{m+1} \frac{(-1)^{m+1-i} e^{\frac{\mathcal{B}_1\mathcal{B}_2}{2}}}{(\mathcal{B}_4-\mathcal{B}_2)^{m+2-i}} \right. \\ & \times \mathcal{B}_1^{-\left(\frac{N_E-i+1}{2}\right)} \mathcal{B}_2^{\frac{N_E-i-1}{2}} \Gamma(N_E) \mathcal{W}_{\frac{1-i-N_E}{2},\frac{i-N_E}{2}}(\mathcal{B}_1\mathcal{B}_2) + \mathcal{B}_4^{N_E-1} e^{\mathcal{B}_1\mathcal{B}_4} \Gamma(N_E) \\ & \left.\left. \times \frac{\Gamma\left(1-N_E, \mathcal{B}_1\mathcal{B}_4\right)}{(\mathcal{B}_2-\mathcal{B}_4)^{m+1}} \right) \right],\end{aligned} \tag{39}$$

where $f_{\gamma_{be}}(.)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{\gamma^{N_E-1}}{\Gamma(N_E)\, \omega_3^{N_E}}\, e^{\frac{-\gamma}{\omega_3}}, \tag{35}$$

where $\Gamma(.)$ is the gamma function, and $f_{\gamma_{je}}(.)$ is given by

$$f_{\gamma_{je}}(\gamma) = \frac{1}{\omega_4} e^{-\frac{\gamma}{\omega_4}}. \tag{36}$$

By substituting (35) and (36) in (34), and after simple algebraic manipulations, $f_{\gamma_E}^{\mathrm{MRC}}(\gamma)$ is obtained as

$$f_{\gamma_E}^{\mathrm{MRC}}(\gamma) = \frac{\gamma^{N_E-1}\, e^{\frac{-\gamma}{\omega_3}}}{\Gamma(N_E)\, \omega_3^{N_E} \omega_4} \sum_{k=0}^{N_E} \binom{N_E}{k} \frac{\Gamma(k+1)}{\left(\frac{\gamma}{\omega_3} + \frac{1}{\omega_4}\right)^{k+1}}. \tag{37}$$

The SOP for MRC, $\mathrm{SOP}_{\mathrm{MRC}}$, is formulated as

$$\mathrm{SOP}_{\mathrm{MRC}} = \int_0^{\infty} F_{\gamma_C}(\beta\gamma + \alpha) f_{\gamma_E}^{\mathrm{MRC}}(\gamma)\, dx. \tag{38}$$

By plugging (50) given in the Appendix and (37) in (38), using partial fraction expansion, then with the help of [41, eq. (1.111)], [41, eq. (3.381.3)], [41, eq. (3.383.10)], and [41, eq. (3.383.4)], $\mathrm{SOP}_{\mathrm{MRC}}$ can be obtained as in (39) at the bottom of the previous page, where $\mathcal{B}_1 = \frac{\beta(q+1)}{\omega_1} + \frac{1}{\omega_3}$, $\mathcal{B}_2 = \frac{\omega_3(k+1)}{\omega_4}$, $\mathcal{B}_3 = \frac{1}{\beta}\left(\alpha + \frac{\omega_1}{\omega_2(q+1)}\right)$, $\mathcal{B}_4 = \frac{1}{\beta}\left(\alpha + \frac{N_J\, \omega_1}{\omega_2(q+1)}\right)$, $\Gamma(.,.)$ is the upper incomplete gamma function [41, eq. (8.350.2)], and $\mathcal{W}_{a,b}(.)$ is the Whittaker function [41, eq. (9.220.4)].

C. ASYMPTOTIC SECRECY OUTAGE ANALYSIS

In this subsection, the SOP at high SNR, i,e., when $\overline{\gamma}_c \to \infty$, is presented to get more insights on the influence of the significant parameters of the proposed system on the performance of the SOP. Specifically, the secrecy diversity order, G_d, and the secrecy array gain, G_a, are investigated. In this case, it is considered that the locations of the BS and C are close. In this scenario, we consider that $\overline{\gamma}_c >> \overline{\gamma}_e$. As $\overline{\gamma}_c \to \infty$, the asymptotic expression of SOP^{∞} can be written as [44]

$$\mathrm{SOP}^{\infty} = (G_a \overline{\gamma}_c)^{-G_d} + \mathcal{O}(\overline{\gamma}_c^{-G_d}), \tag{40}$$

where $\mathcal{O}(.)$ is the higher order terms. From this expression, it can be inferred that the SOP^{∞} curve is characterized by G_d, while the SNR gain of SOP^{∞} relative to the reference curve, $(\overline{\gamma}_c)^{-G_d}$, is characterized by G_a.

1) EAVESDROPPER's CHANNEL WITH SC

To derive the asymptotic SOP for SC, $\mathrm{SOP}_{\mathrm{SC}}^{\infty}$, the exponential function in (50), given in the appendix, is expanded using Taylor series expansion in [41, eq. (1.211.1)]. Then, the first two terms in the expansion are kept, and the higher-order terms are neglected. Thus, the asymptotic CDF of γ_C, $F_{\gamma_C}^{\infty}(.)$, is given by

$$F_{\gamma_C}^{\infty}(\gamma) = \sum_{p=0}^{N_B} \frac{\binom{N_B}{p}\Gamma(p+1)}{\left(\frac{N_J}{\omega_2}\right)^p} \left(\frac{\gamma}{\omega_1}\right)^{N_B} + \mathcal{O}\left(\frac{\gamma}{\omega_1}\right). \tag{41}$$

Now, the $\mathrm{SOP}_{\mathrm{SC}}^{\infty}$ can be obtained using

$$\mathrm{SOP}_{\mathrm{SC}}^{\infty} = (G_{a_{\mathrm{SC}}} \overline{\gamma}_c)^{-G_{d_{\mathrm{SC}}}} + \mathcal{O}(\overline{\gamma}_c^{-G_{d_{\mathrm{SC}}}}), \tag{42}$$

where $G_{d_{\mathrm{SC}}} = N_B$ and the $G_{a_{\mathrm{SC}}}$ is given by

$$\begin{aligned} G_{a_{\mathrm{SC}}} = \Bigg[& \frac{N_E}{\omega_3\omega_4} \sum_{p=0}^{N_B} \binom{N_B}{p} \left(\frac{\omega_2}{N_J}\right)^p \Gamma(p+1) \sum_{k=0}^{N_E-1} (-1)^k \\ & \binom{N_E-1}{m} \sum_{s=0}^{N_B} \binom{N_B}{s} \alpha^{N_B-s} \beta^s e^{-\frac{1}{2\omega_4}} \left(\frac{\omega_3}{k+1}\right)^s \\ & \times\Gamma(s+1) \Bigg(\left(\frac{1}{\omega_4}\right)^{\frac{s-2}{2}} \mathcal{W}_{\frac{-2-s}{2}, \frac{1-s}{2}}\left(\frac{1}{\omega_4}\right) \\ & + \left(\frac{1}{\omega_4}\right)^{\frac{s-1}{2}} \mathcal{W}_{\frac{-1-s}{2}, \frac{-s}{2}}\left(\frac{1}{\omega_4}\right) \Bigg) \Bigg]^{\frac{-1}{N_B}}. \end{aligned}$$

2) EAVESDROPPER's CHANNEL WITH MRC

Using the same approach and following the same steps as above, the asymptotic SOP for MRC, $\mathrm{SOP}_{\mathrm{MRC}}^{\infty}$, can also be written as

$$\mathrm{SOP}_{\mathrm{MRC}}^{\infty} = (G_{a_{\mathrm{MRC}}} \overline{\gamma}_c)^{-G_{d_{\mathrm{MRC}}}} + \mathcal{O}(\overline{\gamma}_c^{-G_{d_{\mathrm{MRC}}}}), \tag{43}$$

where $G_{d_{\mathrm{MRC}}} = N_B$ and $G_{a_{\mathrm{MRC}}}$ is given by

$$\begin{aligned} G_{a_{\mathrm{MRC}}} = \Bigg[& \sum_{p=0}^{N_B} \binom{N_B}{p} \left(\frac{\omega_2}{N_J}\right)^p \Gamma(p+1) \sum_{m=0}^{N_E} \binom{N_E}{m} \\ & \times \frac{\Gamma(m+1)}{\omega_3^{N_E}\, \omega_4\, \Gamma(N_E)} \sum_{s=0}^{N_B} \binom{N_B}{s} \alpha^{N_B-s} \beta^s e^{\frac{1}{\omega_4}} \omega_3^{m+1} \\ & \times \sum_{v=0}^{N_E+s-1} \binom{N_E+s-1}{v} \left(\frac{-\omega_3}{\omega_4}\right)^{N_E+s-v-1} \\ & \times\Gamma\left(v-m, \frac{1}{\omega_4}\right) \omega_3^{v-m} \Bigg]^{\frac{-1}{N_B}}. \end{aligned}$$

D. PROBABILITY OF NON-ZERO SECRECY CAPACITY

In this subsection, the requirement for the presence of the non-zero secrecy capacity is investigated. It is worth noting that the non-zero secrecy capacity is achieved when $\gamma_C > \gamma_E$. From (24), the PNSC is given by

$$\begin{aligned} \Pr(C_S > 0) &= \Pr\left(\frac{1+\gamma_C}{1+\gamma_E} > 1\right) \\ &= 1 - \int_0^{\infty} F_{\gamma_C}(\gamma) f_{\gamma_E}(\gamma)\, d\gamma. \end{aligned} \tag{44}$$

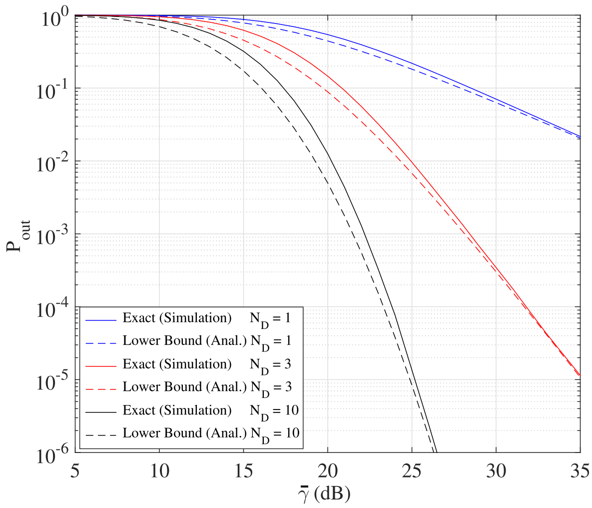


FIGURE 2. The D2D outage probability, P_{out}, vs. SNR, $\bar{\gamma}$, for different number of antennas, N_D, where $\bar{\gamma} = \bar{\gamma}_{tr} = \bar{\gamma}_{rd}$, $\bar{\mu_2} = \bar{\mu_4} = 10$ dB, and $\mathcal{R}_d = 1$ b/s/Hz.

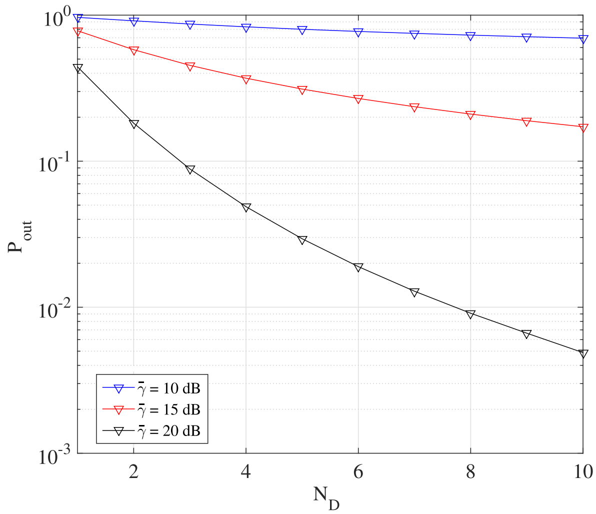


FIGURE 3. The D2D outage probability, P_{out}, vs. N_D for different SNR, $\bar{\gamma}$, where $\bar{\mu_2} = \bar{\mu_4} = 10$ dB, and $\mathcal{R}_d = 1$ b/s/Hz.

1) EAVESDROPPER's CHANNEL WITH SC

By substituting (50) given in the appendix and (31) in (44), and using partial fraction expansion, then [41, eq. (3.352.4)] and [41, eq. (3.353.3)], $\Pr(C_S > 0)_{\text{SC}}$ can be obtained as in (45) at the bottom of this page, where $\mathcal{A}_5 = \frac{s+1}{\omega_1} + \frac{k+1}{\omega_3}$.

2) EAVESDROPPER's CHANNEL WITH MRC

Following the same steps of deriving (45), $\Pr(C_S > 0)_{\text{MRC}}$ can be obtained as in (46) at the bottom of this page, where $\vartheta_1 = \frac{q+1}{\omega_1} + \frac{1}{\omega_3}$, $\vartheta_2 = \frac{\omega_3(k+1)}{\omega_4}$, $\vartheta_3 = \frac{\omega_1}{\omega_2(q+1)}$, and $\vartheta_4 = \frac{N_J\,\omega_1}{\omega_2(q+1)}$.

IV. RESULTS AND DISCUSSIONS

In this section, the analytical results of the D2D outage probability, the SOP, and the PNSC are presented and compared with those obtained by Monte-Carlo simulations. Regarding the described system model, the secrecy performance of the cellular network is analyzed, and the impact of the FD relay is investigated. Without loss of generality, we normalize the variances of the noise at R, D, C, and E to unity.

Fig. 2 plots the analytical lower bound and exact (simulation) outage probability, P_{out}, for D2D communication versus $\bar{\gamma}$, where $\bar{\gamma} = \bar{\gamma}_{tr} = \bar{\gamma}_{rd}$, for different values of N_D at the FD relay. It can be seen that P_{out} of the D2D link decreases

$$
\begin{aligned}
\Pr(C_S > 0)_{\text{SC}} = {} & 1 - \frac{N_E\, N_B}{\omega_3\omega_4} \sum_{k=0}^{N_E-1}\sum_{s=0}^{N_B-1} \frac{(-1)^k}{(k+1)} \binom{N_E-1}{k}\binom{N_B-1}{s} \Bigg[\left(\frac{\omega_3\omega_4}{(k+1)} - N_J \right. \\
& \times \left(\frac{1}{\frac{(k+1)}{\omega_3}N_j - \frac{\mathcal{A}_1}{\omega_4}} \left(\frac{\omega_3\mathcal{A}_2}{(k+1)} e^{\mathcal{A}_2\mathcal{A}_4}\mathrm{Ei}\left[-\mathcal{A}_2\mathcal{A}_5\right] + \frac{1}{\mathcal{A}_4} + \frac{\left(\frac{k+1}{\omega_3}\right)(N_J) - \mathcal{A}_1\left(1+\frac{1}{\omega_4}\right)}{\left(\frac{k+1}{\omega_3}\right)N_j - \frac{\mathcal{A}_1}{\omega_4}} \right.\right. \\
& \left.\left.\left.\times \left(-\frac{\mathrm{Ei}\left[-\mathcal{A}_2\mathcal{A}_5\right]}{e^{-\mathcal{A}_2\mathcal{A}_5}} + \frac{\mathrm{Ei}\left[-\frac{\mathcal{A}_2\, N_J}{\mathcal{A}_1}\right]}{e^{-\frac{\mathcal{A}_2 N_J}{\mathcal{A}_1}}} \right)\right)\right)\right)\Bigg],
\end{aligned} \tag{45}
$$

$$
\begin{aligned}
\Pr(C_S > 0)_{\text{MRC}} = {} & 1 - \frac{N_B}{\Gamma(N_E)\,\omega_3^{N_E}\omega_4} \sum_{m=0}^{N_E}\sum_{q=0}^{N_B-1} \frac{(-1)^q\binom{N_E}{k}\binom{N_B-1}{q}\Gamma(m+1)}{(q+1)} \Bigg[\omega_3^{N_E} e^{\frac{1}{\omega_4}} \sum_{p=0}^{N_E-1} \\
& \binom{N_E-1}{p}\left(\frac{-1}{\omega_4}\right)^{N_E-1-p} \Gamma\left(p-m, \frac{1}{\omega_4}\right) - \frac{N_J\,\omega_1\omega_3^{m+1}}{\omega_2(q+1)} \left(\sum_{i=1}^{m+1}(-1)^{m+1-i} \right. \\
& \times \frac{e^{\frac{\vartheta_1\mathcal{B}_2}{2}}\vartheta_1^{-\left(\frac{N_E-i+1}{2}\right)}\vartheta_2^{\frac{N_E-i-1}{2}}\Gamma(N_E)}{(\vartheta_4-\vartheta_2)^{m+2-i}} \mathcal{W}_{\frac{1-i-N_E}{2},\frac{i-N_E}{2}}(\vartheta_1\vartheta_2) + \vartheta_4^{N_E-1} e^{\vartheta_1\vartheta_4} \\
& \left. \times \frac{\Gamma(N_E)\Gamma\left(1-N_E, \vartheta_1\vartheta_4\right)}{(\vartheta_2-\vartheta_4)^{m+1}} \right) \Bigg],
\end{aligned} \tag{46}
$$

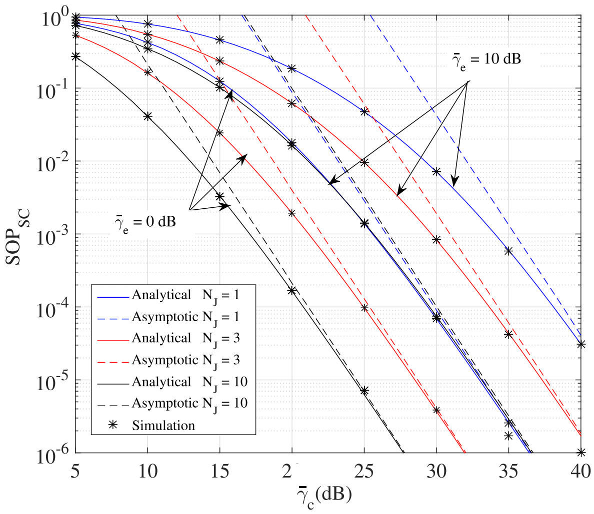


FIGURE 4. **The analytical and Monte-Carlo simulation for the secrecy outage probability, SOP_{SC}, vs. SNR, $\bar{\gamma}_c$, for different $\bar{\gamma}_e$ and N_J, where $\omega_2 = \omega_4 = 10$ dB, $N_B = N_E = 3$, and $\mathcal{R}_s = 1$ b/s/Hz.**

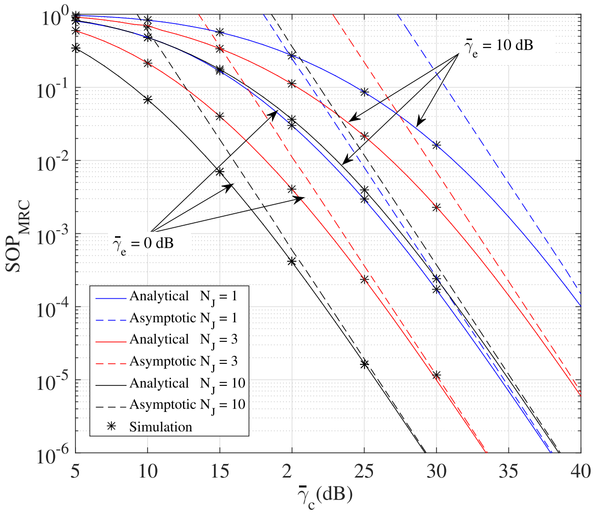


FIGURE 5. **The analytical and Monte-Carlo simulation for the secrecy outage probability, SOP_{MRC}, vs. SNR, $\bar{\gamma}_c$, for different $\bar{\gamma}_e$ and N_J, where $\omega_2 = \omega_4 = 10$ dB, $N_B = N_E = 3$, and $\mathcal{R}_s = 1$ b/s/Hz.**

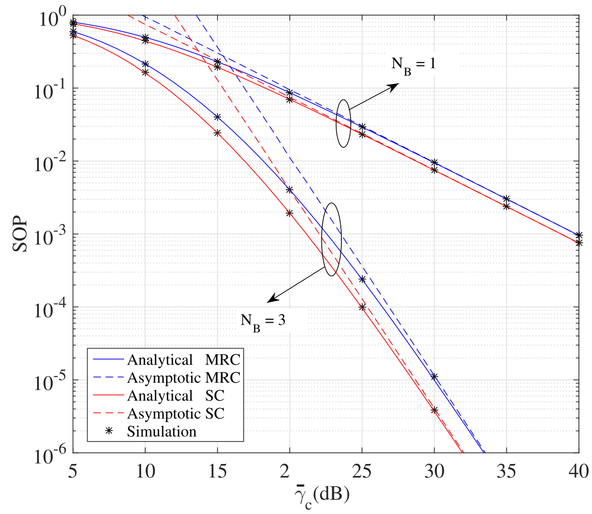


FIGURE 6. **The analytical and Monte-Carlo simulation for the secrecy outage probability, SOP, vs. SNR, $\bar{\gamma}_c$, for different N_B, where $\omega_2 = \omega_4 = 10$ dB, $N_J = N_E = 3$, $\bar{\gamma}_e = 0$ dB, and $\mathcal{R}_s = 1$ b/s/Hz.**

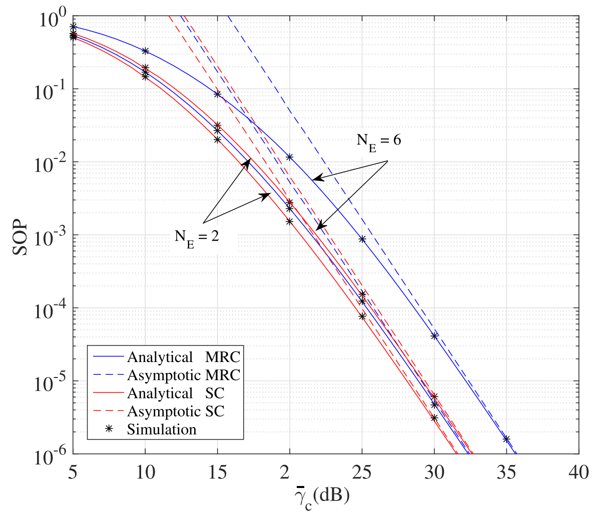


FIGURE 7. **The analytical and Monte-Carlo simulation for the secrecy outage probability, SOP, vs. SNR, $\bar{\gamma}_c$, for different N_B, where $\omega_2 = \omega_4 = 10$ dB, $N_J = N_E = 3$, $\bar{\gamma}_e = 0$ dB, and $\mathcal{R}_s = 1$ b/s/Hz.**

monotonically as $\bar{\gamma}$ increases, and there is no any outage floor. Notably, the P_{out} improves significantly with increasing N_D. Thus, the data transmission of D2D communication improves as a result of utilizing the MIMO relay as compared to a single relay. Furthermore, it can be observed that simulation and numerical results match at high SNR, confirming the tightness of the lower bound in (13) in this regime.

To evaluate the impact of the MIMO relay on the reliability in the D2D communication, Fig. 3 presents P_{out} versus N_D, for different values of $\bar{\gamma}$. As such, the effect of N_D on the D2D performance is examined, where P_{out} is seen to improve continuously with increasing N_D and $\bar{\gamma}$ as expected.

The SOP for selection combining, SOP_{SC}, of the cellular network is plotted in Fig. 4 versus $\bar{\gamma}_c$, for different $\bar{\gamma}_e$ and N_J. The SNR at E, $\bar{\gamma}_e$, takes two possible values: 0 dB and 10 dB while $\mathcal{R}_s$ is set at 1 b/s/Hz and $N_B = N_E = 3$. It can be noted that the SOP_{SC} decreases as N_J increases, illustrating the impact of the jamming signals on E. As a result, secure data transmission is guaranteed. Additionally, the SOP_{SC} increases as $\bar{\gamma}_c$ decreases, and $\bar{\gamma}_e$ increases. Besides, the asymptotic curves are depicted, and a very good match with the exact analysis is seen as $\overline{\gamma}_c \to \infty$. Most noteworthy in the asymptotic curves is the fact that they precisely predict G_a and G_d. Furthermore, the numerical and the simulation results match perfectly, verifying the accuracy of our analysis. Interesting, the SOP_{SC} of the cellular network decreases as a result of using the FD jamming MIMO relay.

In Fig. 5, the secrecy outage probability for maximum ratio combining, SOP_{MRC}, of the cellular network is plotted using the same parameters as in Fig. 4. It can be seen that SOP_{MRC} decreases with increasing N_J, implying an improvement in the security level of the cellular network. From Figs. 4 and 5, we can note that the secrecy performance of the cellular network is lower when E employs the MRC as compared to

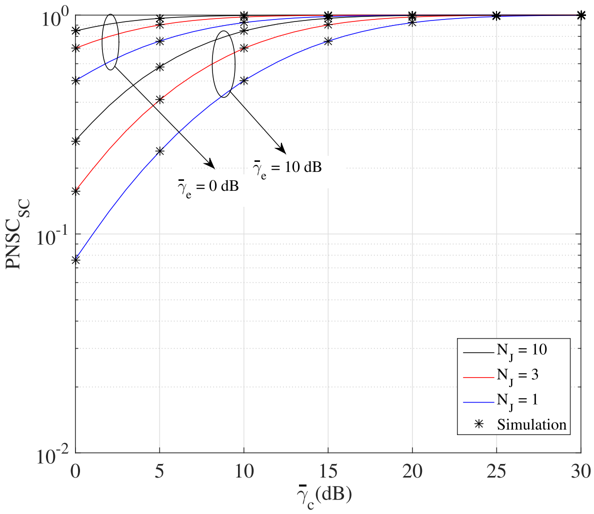


FIGURE 8. The analytical and Monte-Carlo simulation for the probability of non-zero secrecy outage probability, PNSC_{SC}, vs. SNR, $\bar{\gamma}_c$, for different $\bar{\gamma}_e$ and N_J, where $\omega_2 = \omega_4 = 10$ dB, $N_B = N_E = 3$, and $\mathcal{R}_S = 1$ b/s/Hz.

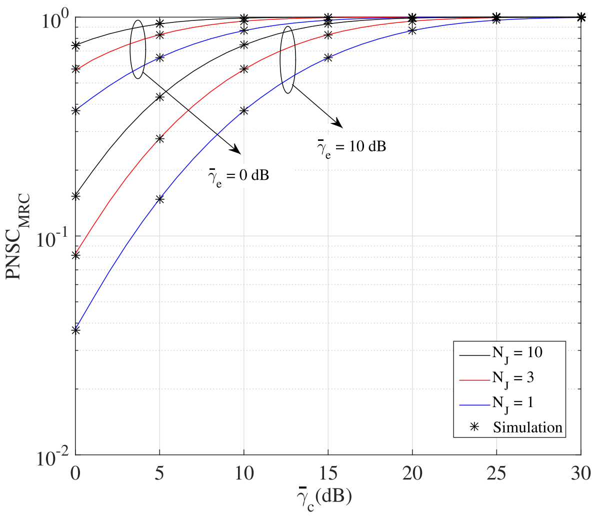


FIGURE 9. The analytical and Monte-Carlo simulation for the probability of non-zero secrecy outage probability, PNSC_{MRC}, vs. SNR, $\bar{\gamma}_c$, for different $\bar{\gamma}_e$ and N_J, where $\omega_2 = \omega_4 = 10$ dB, $N_B = N_E = 3$, and $\mathcal{R}_S = 1$ b/s/Hz.

the SC technique. This can be described by the fact that the MRC provides the best SNR gain at E over the SC scheme.

Figures 6 and 7 show the SOP versus $\bar{\gamma}_c$ where the analytical results for both SC and MRC are given by (33) and (39), respectively. Additionally, the asymptotic SOP results for both SC and MRC are also presented. In Fig. 6, there is an increase in the SOP for both SC and MRC with decreasing N_B because the cellular capacity, C_C, increases with increasing N_B. This can be explained by the fact that G_a increases with N_B. In Fig. 7, there is an increase in the SOP for both SC and MRC with increasing N_E. Since the diversity order is not influenced by N_E, the increase in the SOP is due to the array gain. From Figs. 6 and 7, it can be confirmed that the SOP for both SC and MRC has the same secrecy diversity orders N_B.

Figures 8 and 9 plot the PNSC versus $\bar{\gamma}_c$ where (45) and (46) are used for the analytical results of SC and MRC, respectively. From these figures, it is obvious that the PNSC increases as $\bar{\gamma}_c$ increases for a fixed $\bar{\gamma}_e$. Additionally, the PNSC increases with decreasing $\bar{\gamma}_e$. Moreover, it can also be noted that the PNSC increases as N_J increases. It is worth mentioning that even when the average SNR of the main channel, $\bar{\gamma}_c$, is lower than that of the eavesdropper's channel, $\bar{\gamma}_e$, the PNSC exists. Interestingly, for the SC technique, the PNSC is lower than that of the MRC technique. Analytical results are also found to match the simulation results, validating the correctness of our analysis.

V. CONCLUSION

In this paper, a cooperative scheme is proposed to improve the secrecy performance of the cellular network and the reliability of the D2D communications simultaneously. To this end, an FD MIMO relay is employed to confuse the eavesdropper by generating jamming signals, while ensuring improved transmission performance for the D2D system. At E, two practical combining techniques, SC or MRC, are utilized to combine the wiretapped signals. Considering a practical scenario in which the CSI of the eavesdropper's channel is unknown, a dual antenna selection scheme at the relay is proposed. A comprehensive analysis is undertaken to evaluate the performance of the proposed system model, and new closed-form expressions for the D2D outage probability, the cellular SOP, and the cellular PNSC are derived. To gain more insights into the effect of the various system parameters on the SOP, an asymptotic analysis is carried out. This analysis reveals that the same diversity order of N_B is achieved for both SC and MC techniques. It is also observed that the diversity order is not influenced by N_E. Moreover, we confirmed that, under these combining techniques, increasing N_J and N_B enhances the secrecy performance of the cellular network. Finally, numerical results are found to agree very well with simulation results, confirming our analysis. As revealed by the analytical and simulation results, the SOP and the D2D outage probability are simultaneously improved, confirming the benefits of the cooperation.

APPENDIX
DERIVATION OF THE SECRECY OUTAGE PROBABILITY

To derive the PDF of γ_C, we have [40]

$$F_{\gamma_C}(\gamma) = \int_0^\infty F_{\gamma_{bc}}(\gamma(\xi+1)) f_{\gamma_{jc}}(\xi)\, d\xi, \tag{47}$$

where $F_{\gamma_{bc}}(.)$ is given by

$$F_{\gamma_{bc}}(\gamma) = N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left(1 - e^{-\frac{\gamma(k+1)}{\omega_1}}\right). \tag{48}$$

The jamming antenna is selected based on the minimum interference generated from R_j towards C. Hence, $f_{\gamma_{jc}}(.)$ is given by

$$f_{\gamma_{jc}}(\gamma) = \frac{N_J}{\omega_2} e^{-\frac{N_J \gamma}{\omega_2}}. \tag{49}$$

Now, by plugging (48) and (49) into (47), and after simple algebraic manipulations, one can gets

$$F_{\gamma_C}(\gamma) = N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left(1 - \frac{N_j\, e^{-\frac{\gamma(k+1)}{\omega_1}}}{N_j + \frac{\omega_2 \gamma(k+1)}{\omega_1}}\right). \tag{50}$$

By plugging (50) and (31) into (32), and utilizing partial fraction expansion, then [41, eq. (3.352.4)] and [41, eq. (3.353.3)], the $\mathrm{SOP_{SC}}$ can be obtained as in (33).

REFERENCES

[1] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, "A survey of Device-to-Device communications: Research issues and challenges," *IEEE Commun. Surveys Tutr.*, vol. 20, no. 3, pp. 2133–2168, 3rd Quart., 2018.

[2] A. Asadi, Q. Wang, and V. Mancuso, "A survey on Device-to-Device communication in cellular networks," *IEEE Commun. Surveys Tutr.*, vol. 16, no. 4, pp. 1801–1819, Apr. 2014.

[3] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-Device communication in LTE-advanced networks: A survey," *IEEE Commun. Surveys Tutr.*, vol. 17, no. 4, pp. 1923–1940, Dec. 2015.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[5] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[6] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[7] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an Amplify-and-Forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[8] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[9] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[10] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[11] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure Amplify-and-Forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[13] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[14] H. Lei, Z. Yang, K.-H. Park, I. S. Ansari, Y. Guo, G. Pan, and M.-S. Alouini, "Secrecy outage analysis for cooperative NOMA systems with relay selection schemes," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6282–6298, Sep. 2019.

[15] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.

[16] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[17] H. Lei, J. Zhang, K.-H. Park, P. Xu, Z. Zhang, G. Pan, and M.-S. Alouini, "Secrecy outage of max–min TAS scheme in MIMO-NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, Aug. 2018.

[18] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for Device-to-Device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[19] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for Device-to-Device communication: A physical layer security perspective," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, Apr. 2018.

[20] W. Wang, K. C. Teh, and K. H. Li, "Enhanced physical layer security in D2D spectrum sharing networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106–109, Feb. 2017.

[21] F. Alavi, N. M. Yamchi, M. R. Javan, and K. Cumanan, "Limited feedback scheme for Device-to-Device communications in 5G cellular networks with reliability and cellular secrecy outage constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8072–8085, Sep. 2017.

[22] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, "Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5766–5777, Jul. 2018.

[23] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[24] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.

[25] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, pp. 1195–1206, May 2017.

[26] H.-M. Wang, B.-Q. Zhao, and T.-X. Zheng, "Adaptive full-duplex jamming receiver for secure D2D links in random networks," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1254–1267, Feb. 2019.

[27] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan. 2019.

[28] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, "On the physical layer security of underlay multihop Device-to-Device relaying," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.

[29] J. M. Moualeu, T. M. N. Ngatched, and D. B. da Costa, "Sequential relay selection in D2D-enabled cellular networks with outdated CSI over mixed fading channels," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 245–248, Feb. 2019.

[30] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, "Enhancing physical layer security using underlay full-duplex relay-aided D2D communications," in *Proc. IEEE Wireless Commun. NetW. Conf. (WCNC)*, Apr. 2020, pp. 1–7.

[31] C. Ren, H. Zhang, J. Wen, J. Chen, and C. Tellambura, "Successive two-way relaying for full-duplex users with generalized self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 63–76, Jan. 2019.

[32] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.

[33] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.

[34] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for mimo underlay cognitive radio systems over nakagami-*m* channels," *IEEE Trans. Veh. Tech.*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[35] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[36] I. Krikidis, J. Thompson, S. Mclaughlin, and N. Goertz, "Max-min relay selection for legacy amplify-and-forward systems with interference," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 3016–3027, Jun. 2009.

[37] A. Ghasemi and E. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.

[38] S. S. Ikki and S. Aissa, "Performance analysis of two-way Amplify-and-Forward relaying in the presence of co-channel interferences," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 933–939, Apr. 2012.

[39] M. Li, L. Bai, Q. Yu, and J. Choi, "Optimal beamforming for dual-hop MIMO AF relay networks with cochannel interferences," *IEEE Trans. Signal Process.*, vol. 65, no. 7, pp. 1825–1840, Apr. 2017.

[40] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.

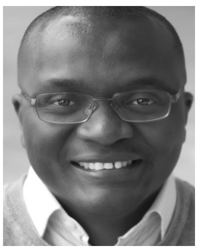
[41] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2014.

[42] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[43] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[44] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

MAJID H. KHOSHAFA (Student Member, IEEE) received the B.Sc. degree in communication engineering from Ibb University, Ibb, Yemen, in 2007, and the M.Sc. degree in telecommunications engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in 2017. He is currently pursuing the Ph.D. degree with the Memorial University of Newfoundland, St. John's, NL, Canada. From 2009 to 2010, he worked as a Radio Network Planning and Optimization Engineer with MTN Telecommunications, Sana'a, Yemen. He was a Researcher and Teaching Assistant with the Electrical Department, Faculty of Engineering, Ibb University, from 2010 to 2013. His research interests include wireless communications, physical layer security, 5G enabling technologies, D2D communications, and cognitive radio.



TELEX M. N. NGATCHED (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics from the University of Yaoundé, Cameroon, in 1992 and 1993, respectively, the M.Sc. (Eng.) degree *(cum laude)* in electronic engineering from the University of Natal, Durban, South Africa, in 2002, and the Ph.D. degree in electronic engineering from the University of KwaZulu-Natal, Durban, South Africa, in 2006. From July 2006 to December 2007, he was with the University of KwaZulu-Natal as a Postdoctoral Fellow, and from 2008 to 2012, with the Department of Electrical and Computer Engineering, University of Manitoba, Canada, as a Research Associate. In August 2012, he joined the Memorial University of Newfoundland, where he is currently an Associate Professor and Coordinator of the Engineering One Program at Grenfell Campus. His research interests include 5G enabling technologies, visible light communications, power-line communications, optical communications, and underwater communications.

Dr. Ngatched was a recipient of the Best Paper Award at the IEEE Wireless Communications and Networking Conference (WCNC) in 2019. He was the Publication Chair of the IEEE CWIT 2015, an Associate Editor of the IEEE Communications Letters, from 2015 to 2019, and a Technical Program Committee (TPC) Member and a Session Chair for many prominent IEEE conferences including IEEE GLOBECOM, IEEE ICC, IEEE WCNC, IEEE VTC, and IEEE PIMRC. He serves as the Managing Editor for the IEEE Communications Letters and as an Associate Editor for the IEEE Open Journal of the Communications Society. He is a Professional Engineer (P.Eng.) registered with the Professional Engineers and Geoscientists of Newfoundland and Labrador, St. John's, NL, Canada.

MOHAMED H. AHMED (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Carleton University, Ottawa, in 2001. From 2001 to 2003, he worked as a Senior Research Associate with Carleton University. In 2003, he joined the Faculty of Engineering and Applied Science, Memorial University, where he has worked as a Full Professor until December 2019 and as an Adjunct Professor from January 2020. He is currently an LTA Professor with the University of Ottawa. He has published more than 155 articles in international journals and conferences. His research is sponsored by NSERC, CFI, QNRF, Bell/Aliant and other governmental and industrial agencies. His research interests include radio resource management in wireless networks, multihop relaying, cooperative communication, vehicular ad-hoc networks, cognitive radio networks, and wireless sensor networks. He served as a Co-Chair for the Signal Processing Track in ISSPIT'14 and served as a Co-Chair for the Transmission Technologies Track in VTC'10-Fall, and the Multimedia and Signal Processing Symposium, in CCECE'09. He received the Ontario Graduate Scholarship for Science and Technology, in 1997, the Ontario Graduate Scholarship, in 1998, 1999, and 2000, and the Communication and Information Technology Ontario (CITO) Graduate Award, in 2000. He served as an Editor for the IEEE Communication Surveys and Tutorials, from 2007 to 2018, and as a Guest Editor of a special issue on Fairness of Radio Resource Allocation, EURASIP JWCN, in 2009, and as a Guest Editor of a special issue on Radio Resource Management in Wireless Internet, *Wireless and Mobile Computing* Journal (Wiley), 2003. He is a registered Professional Engineer (P.Eng.) in the province of Newfoundland, Canada.

AHMED IBRAHIM (Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics and communications engineering from the Arab Academy for Science, Technology and Maritime Transport, Egypt, in 2006 and 2010, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba (UoM), in October 2016. He was a Faculty Member Teaching Assistant with the Arab Academy for Science, Technology and Maritime Transport, where he was also an Assistant Lecturer from September 2006 to July 2011. He was a Postdoctoral Fellow and a senior per course Instructor with the Memorial University of Newfoundland from September 2016 to August 2019 and from September 2018 to December 2019, respectively. He taught courses in communication networks and wireless communications. He has coauthored a book entitled *Optimization Methods for User Admissions and Radio Resource Allocation for Multicasting over High Altitude Platforms* (River Publishers, February 2019). His research area covers, but is not limited to AI enabled PHY, Faster-than-Nyquist Signalling, radio resource allocation, cross-layer design and optimization, device-to-device communications, link adaptation, heterogeneous networks, backhauling using millimeter technology, network performance analysis, UAV HAP communications, wireless sensor networks, scheduling for video streaming, 5G enabling technologies, edge computing, visible light communications, heterogeneous cellular networks, and millimeter backhauling. He was a recipient of the Best Paper Award from the IEEE Wireless Communications and Networking Conference (WCNC), in 2019. He received the IGSES and IGSS Scholarships from UoM. He is currently an Associate Editor in the IEEE Open Journal of the Communications Society (IEEE OJ-COMS). He also serves as a TPC Member and a Reviewer for a number of IEEE journals and conferences, such as the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE Communication Letters, the IEEE Systems Journal, IEEE Access, IEEE JSTSP, IEEE GLOBECOM, IEEE ICC, IEEE VTC, and IEEE COMNETSAT. He was awarded as an Exemplary Reviewer of the IEEE Communications Letters journal in 2017.